IN THE CLAIMS:

1. (currently amended) A smart card applications network for ~~smart card applications using~~ use with a smart card terminal in combination with a smart card ~~terminal~~ containing memory-economizing data pointers, said smart card applications network comprising:

a communications network in operative communication with said smart card terminal; and

a central database server in operative communication with said communications network~~, said central database server~~ and including a plurality of partitioned memory locations wherein at least one of said partitioned memory locations contains information associated with an authorized user of said smart card[[,]];

whereby said information ~~being~~ is accessible ~~by~~ through said smart card terminal via at least one of said memory-economizing data pointers contained within said smart card.

2. (currently amended) The smart card applications network of claim 1 further comprising a central time/date authority in operative communication with said communications network, said central time/date authority providing a time verification that is associated with said information as transmitted between said central database server and said smart card terminal.

3. (currently amended) The smart card applications network of claim 1 wherein said communications network is part of a public-switched telephone network.

4. (currently amended) The smart card applications network of claim 1 wherein said communications network communicates with said smart card terminal via the plain old telephone system (POTS).

5. (currently amended) The smart card applications network of claim 1 wherein said communications network includes the Internet.

6. (currently amended) The smart card applications network of claim 1 wherein said central database server comprises a network smart card server and a plurality of interconnected database servers.

7. (currently amended) The smart card applications network of claim 1 wherein at least one of said ~~plurality of~~ partitioned memory locations includes both a restricted data portion containing information regarding said authorized user that is accessible to a first predetermined group of network users[[,]] and a public data portion containing information regarding said authorized user that is accessible to a second predetermined group of network users.

8. (currently amended) The smart card applications network of claim ~~2~~ 1 further comprising a central time/date authority in operative communication with said communications network, said central time/date authority providing a time verification that is associated with said information as transmitted between said central database server and said smart card terminal;

wherein at least one of said ~~plurality of~~ partitioned memory locations includes both a restricted data portion containing information regarding said authorized user that is accessible to a first predetermined group of network users[[,]] and a public data portion containing information regarding said authorized user that is accessible to a second predetermined group of network users.

9. (currently amended) The smart card applications network of claim ~~7~~ 1 wherein at least one of said partitioned memory locations includes both a restricted data portion containing information regarding said authorized user that is accessible to a first predetermined group of network users and a public data portion containing information regarding said authorized user that is accessible to a second predetermined group of network users; and

wherein each of said ~~plurality of~~ partitioned memory locations supports a different smart card application.

10. (currently amended) A method of ~~accessing~~ providing access to information relating to an authorized user of a smart card for executing a smart card transaction, said method comprising the steps of:

providing at least one smart card terminal for ~~connection~~ receiving and communicatively interacting with ~~a~~ said smart card;

~~selecting~~ verifying authorization for a desired ~~authorized~~ application that is selected at said smart card terminal for said smart card transaction;

transmitting ~~through a communications network~~ at least an authorization code associated with said smart card both through a communications network and to a network smart card server~~, said network smart card server including~~ that includes a plurality of application-specific partitioned memory locations[[,]];

utilizing at least one data pointer provided by said authorization code ~~providing a data pointer pointing~~ to point to information relating to said authorized user that is contained in at least one of said ~~plurality of~~ application-specific partitioned memory locations; and

transmitting said information through said communications network to said smart card terminal.

11. (currently amended) The method of claim 10 further comprising the steps of:

modifying said information as accessed at said smart card terminal[[,]];

~~re-transmitting~~ transmitting said ~~modified~~ information as modified to said network smart card server[[,]]; and

storing said ~~modified~~ information as modified in ~~said~~ at least one of said ~~plurality of~~ application-specific partitioned memory locations.

12. (currently amended) The method of claim 10 further comprising the step of providing a central time/date value that is associated with said ~~transmitted~~ information as transmitted.

13. (currently amended) The method of claim 10 further comprising the ~~step~~ steps of:

modifying ~~the~~ information relating to said authorized user; and

~~stored~~ storing said information as modified on said smart card.

14. (currently amended) A network smart card server for use in smart card transactions, said network smart card server comprising:

a first plurality of application-specific partitioned memory locations containing information relating to an authorized user of a smart card;

a second plurality of application-specific partitioned memory locations containing further information ~~of~~ relating to said authorized user; and

a microprocessor programmed to receive an authorization code associated with said smart card, said authorization code representing ~~a~~ at least one data pointer for pointing to ~~said~~ authorized ~~user's~~ user related information contained within ~~a~~ at least one memory location within said first plurality or said second plurality of application-specific partitioned memory locations.

15. (currently amended) The network smart card server of claim 14 wherein said information contained in ~~each of~~ said first plurality of application-specific partitioned memory locations ~~represents~~ is access-designated public data ~~associated with~~ for said smart card ~~transaction~~ transactions.

16. (currently amended) The network smart card server of claim 15 wherein said information contained in ~~each of~~ said second plurality of application-specific partitioned memory locations ~~represents~~ is access-designated restricted data ~~associated with~~ for said smart card ~~transaction~~ transactions.

17. (currently amended) The network smart card server of claim 14 wherein each of said first plurality and said second plurality of application-specific partitioned memory locations ~~contain~~ contains information ~~corresponding to a~~ designated for at least one smart card application.

18. (currently amended) The network smart card server of claim 14 wherein at least one of said first plurality of application-specific partitioned memory locations is located on a separate database server accessible through a communications network.

19. (original) The network smart card server of claim 18 wherein said communications network includes the Internet.

20. (original) The network smart card server of claim 18 wherein said communications network includes a public-switched telephone network.